

# Ativação 2FA/MFA

## (Duplo Fator de Autenticação / *MultiFactor Authentication*)

Há diferença entre a autenticação com APP ou com SMS. A autenticação via APP acaba por ser mais robusta caso haja falha na rede móvel no telemóvel.

1º Método - APP Microsoft Authenticator (pág. 2)

2º Método - Via SMS (pág. 12)

# APP Microsoft

# Authenticator

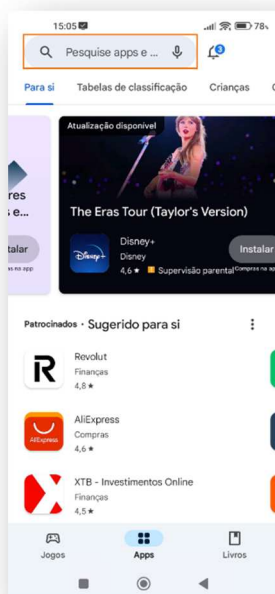
*Departamento Sistemas de Informação*

Gandra, 28 de março de 2024

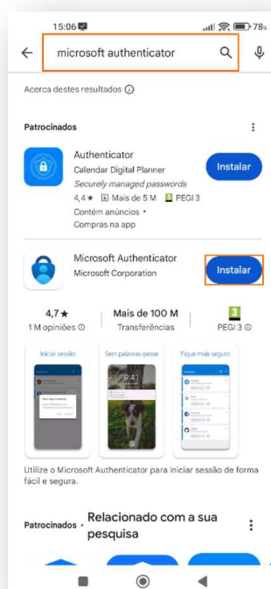
1. Aceder à *Play Store* da *Google* no caso de Telemóvel com Sistema Operativo Android (ex: Samsung, Xiaomi, etc), ou aceder *Apple Store* no caso de Telemóvel iPhone.



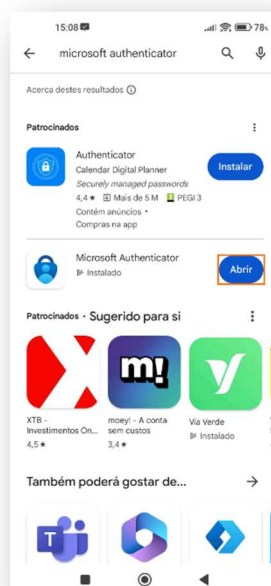
2. No campo de pesquisa, procurar pela **APP Microsoft Authenticator**...



3. Instalar a **APP Microsoft Authenticator** – Clicar no botão “Instalar”;



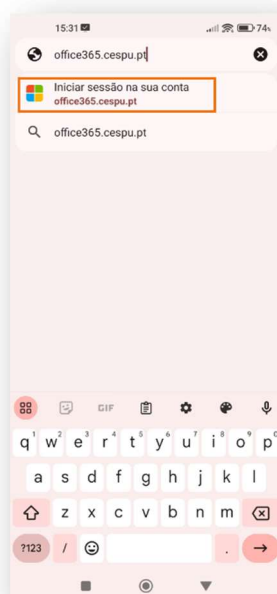
4. Concluído o processo de instalação, deverá abrir a APP clicando no botão “Abrir”;



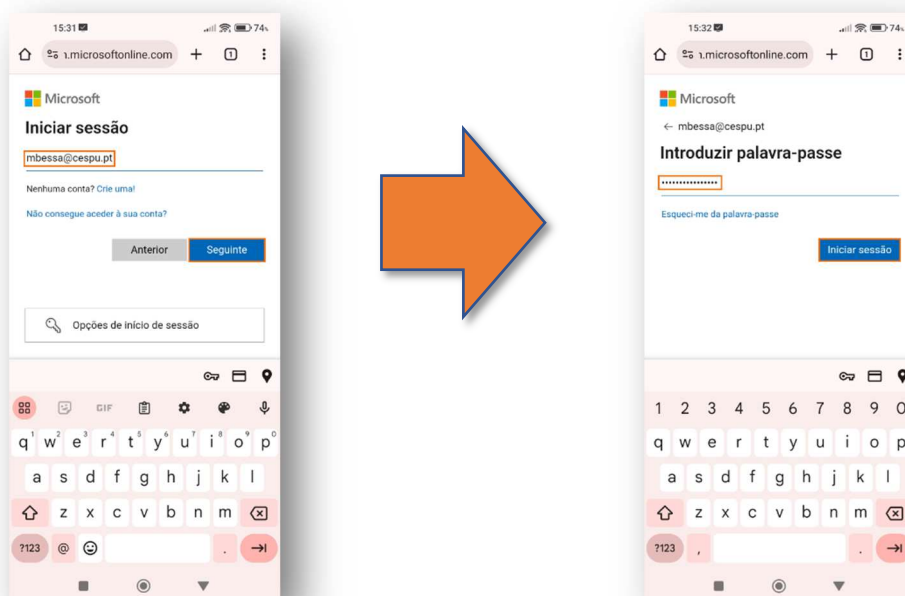
5. Em seguida, deverá permitir que a APP lhe envie notificações, clicando no botão “Permitir”;



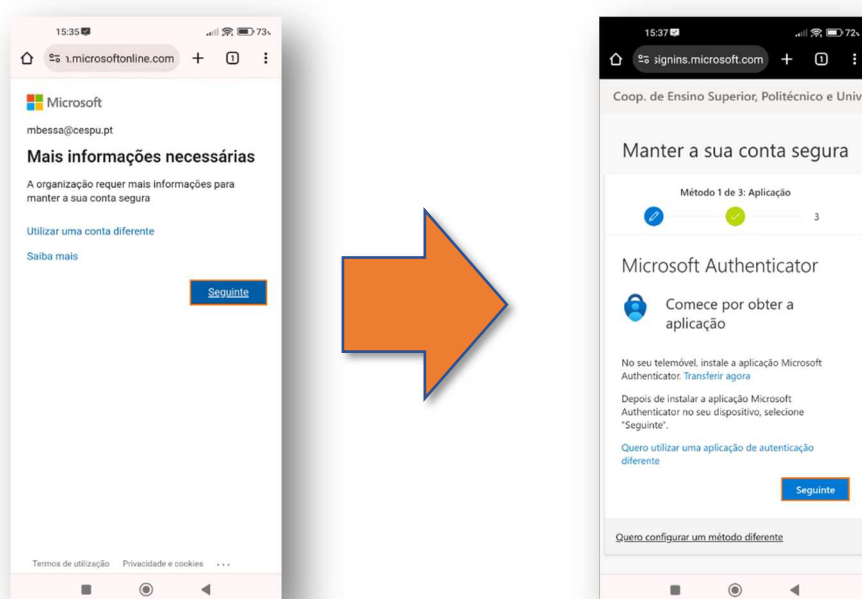
6. Após permitir as notificações, deverá clicar no botão “Aceitar” e em seguida clicar no botão “Continuar”;
7. Seguidamente, no canto superior direito do ecrã clicar no botão “Ignorar”;
8. No passo seguinte deverá abrir um separador no navegador (*browser*) de internet e aceder ao *site* office365.cespu.pt e colocar as credenciais – email institucional e palavra-passe;



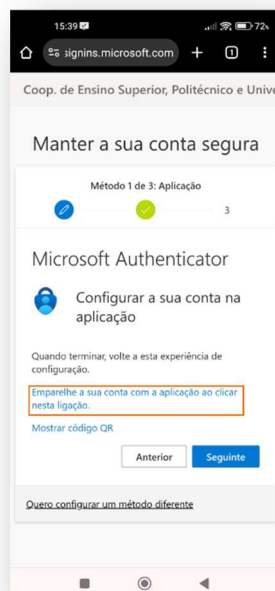
9. Após colocar as credenciais de acesso à conta institucional, clicar no botão “Seguinte” para continuar a configuração do mecanismo 2FA;



10. De seguida, é pedido no *site* para se proceder à instalação da **APP Microsoft Authenticator**, mas como já se encontra instalada, clicar no botão “Seguinte”;



11. Clicar na opção "Emparelhe a sua conta com a aplicação ao clicar nesta ligação";



12. Em seguida aparecerá um mecanismo automático que associa a conta institucional à APP. Quando este mecanismo finaliza com sucesso aparece a seguinte notificação, pelo que deverá ser clicado no botão "Ok".



13. Voltar ao separador no navegador e clicar no botão “Seguinte” e aparecerá um número de confirmação...

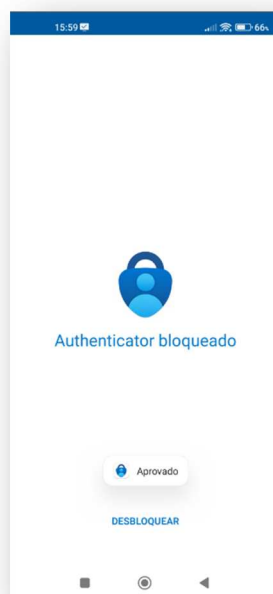


... que deverá ser introduzido na **APP Microsoft Authenticator**. **Nota:** Este número é sempre variável...

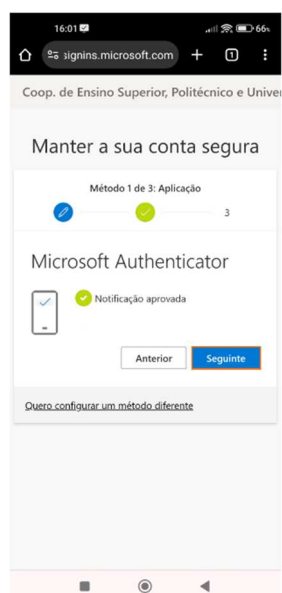




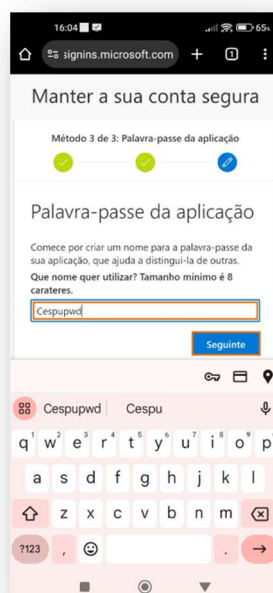
... após clicar em “Sim” na APP poderá ser necessário validar com o método de desbloqueio do Telemóvel (PIN ou leitura digital).



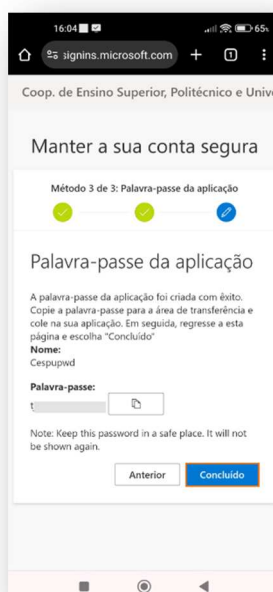
14. Após confirmar o número na APP, no separador do navegador clicar no botão “Seguinte”.



15. Definir o nome para a palavra-passe da aplicação (exemplo – Cespupw0d!) e clicar no botão “Seguinte”.



16. Por último, aparece uma password gerada para proteger a aplicação que deve ser guardada (para fins de recuperação de conta)...



... e de seguida clicar no botão “Concluído”.



Após a execução deste conjunto de passos o processo de ativação de 2FA/MFA encontra-se concluído, pelo que, a partir desse momento, sempre que utilizar o email institucional pela primeira vez numa aplicação, plataforma ou dispositivo, será enviado para a **APP Microsoft Authenticator** um número de confirmação.

**NOTA:** Em caso de dúvidas na configuração do “2FA/MFA – Duplo Fator de Autenticação” deve evitar a memorização de palavras-chave.

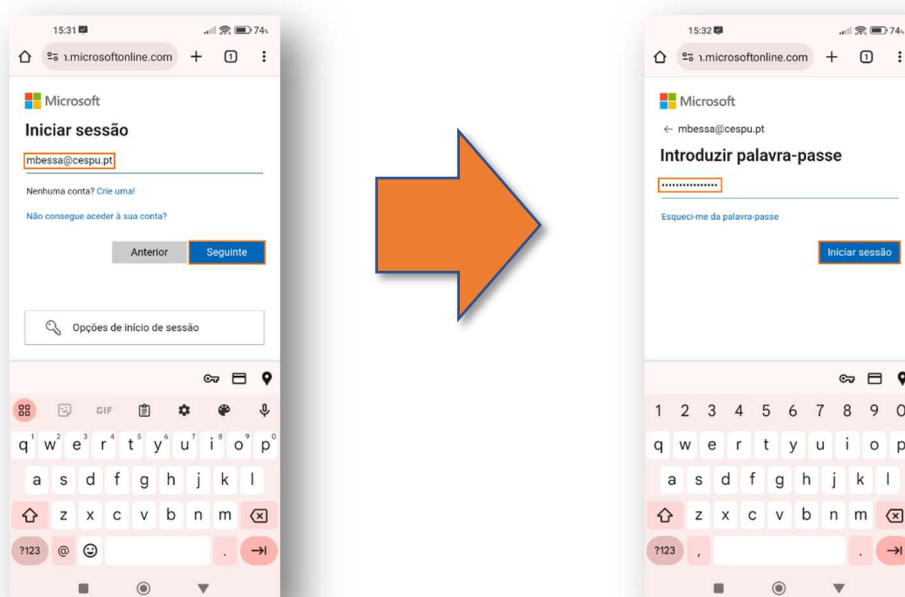
# Via SMS da

# Microsoft

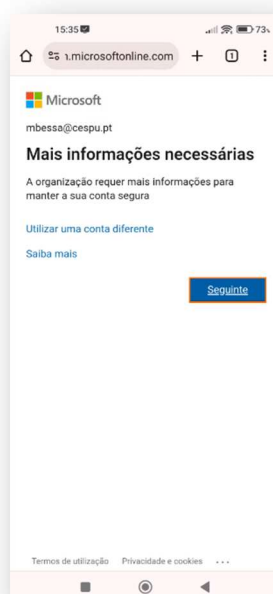
*Departamento Sistemas de Informação*

Gandra, 28 de março de 2024

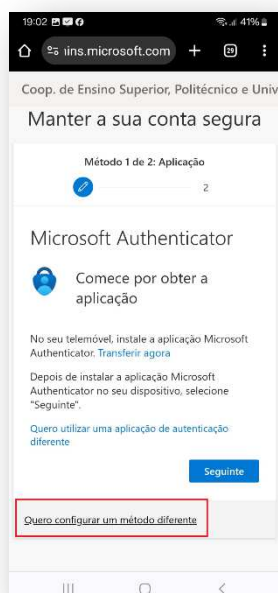
1. Aceder ao portal “<https://portal.office.com>” e colocar as credenciais de acesso compostas pelo login correspondente à conta institucional (ex: [A33333@alunos.cespu.pt](mailto:A33333@alunos.cespu.pt), [gervasio.martins@ipsn.cespu.pt](mailto:gervasio.martins@ipsn.cespu.pt), [gervasio.martins@iucs.cespu.pt](mailto:gervasio.martins@iucs.cespu.pt), [mbessa@cespu.pt](mailto:mbessa@cespu.pt)) e respetiva palavra-passe de acesso aos computadores / Rede wireless;



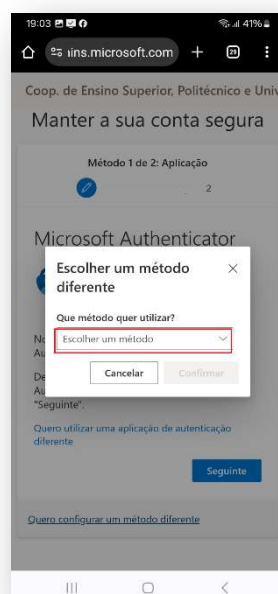
2. Seguidamente, clicar no botão “Iniciar Sessão” e no ecrã que se segue em **Seguinte**...



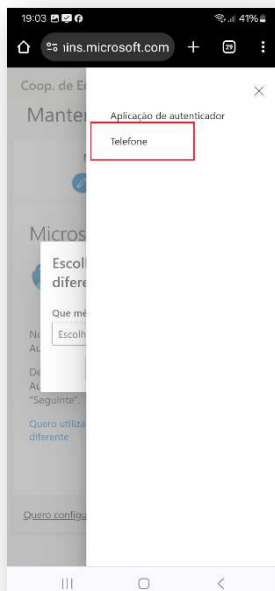
- Neste ecrã deverá clicar na opção que se encontra no fundo com a designação “Quero configurar um método diferente”...



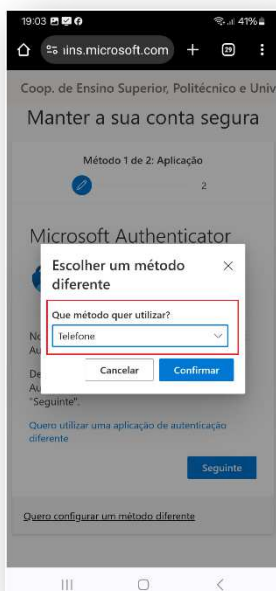
- No ecrã que se segue deverá clicar no campo “Que método quer utilizar”...



5. Na janela de diálogo que é apresentada, deverá selecionar **"Telefone"**...

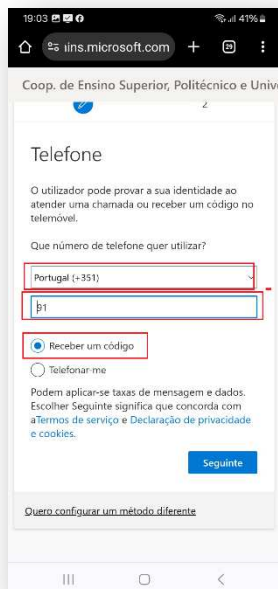


6. O campo **"Que método quer utilizar"** ficará preenchido com o dado...



7. Seguidamente, deverá preencher cada um dos campos assinalados a vermelho com os dados que se pretende. A título de exemplo, um utilizador que tem cartão SIM (Operadora de telecomunicações) portuguesa, deverá indicar o país a que a mesma pertence **Portugal - (+351)**, o número que possuiu

(ex: 91 123 456 7) e a opção **“Receber um código”**, pois irá ser enviado um código composto por 6 algarismos por SMS para o telemóvel indicado...



8. Na janela que se segue deverá indicar o código que entretanto recebeu por SMS...





9. ... o código na SMS é apresentado na seguinte forma...



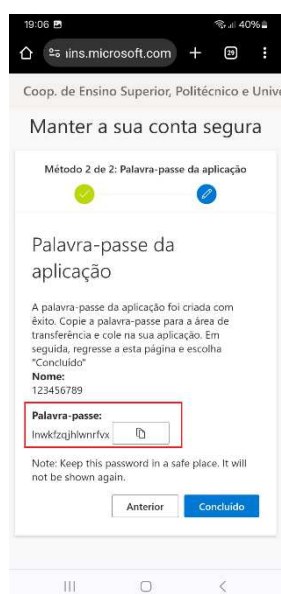
10. Caso o código seja corretamente introduzido o seguinte ecrã será apresentado...



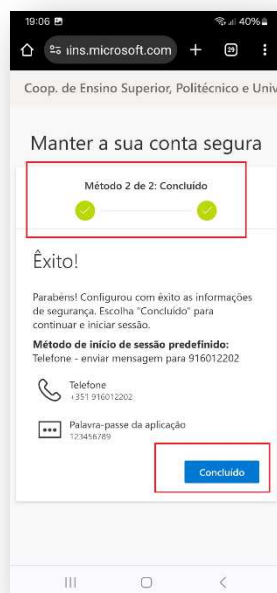
11. Definir o nome para a palavra-passe da aplicação (exemplo – Cespupw0d!) e clicar no botão “Seguinte”.



12. Por último, aparece uma password gerada para proteger a aplicação que deve ser guardada (para fins de recuperação de conta)...



... e de seguida clicar no botão “Concluído”.



Após a execução deste conjunto de passos o processo de ativação de 2FA/MFA encontra-se concluído, pelo que, a partir desse momento, sempre que utilizar o email institucional pela primeira vez numa aplicação, plataforma ou dispositivo, será enviado uma SMS da *Microsoft* um número de telemóvel que indicou no seu registo.

**NOTA:** Em caso de dúvidas na configuração do “2FA/MFA – Duplo Fator de Autenticação” deve evitar a memorização de palavras-chave.